WHAT IS CLAIMED IS:

1. A method of secure PIN processing in a network transaction comprising the steps of:

sending terminal data to a terminal;

receiving corollary data generated from user input and terminal data from said terminal;

sending corollary data and HSM data to a hardware security module;

receiving a PIN block generated from corollary data and HSM data from said hardware security module.

2. The method of claim 1, wherein said terminal data includes algorithms.

3. The method of claim 1, wherein said terminal data includes seed data.

4. The method of claim 1, wherein said user input includes cursor location data.

5. The method of claim 1, further comprising the step of receiving transaction data.

6. The method of claim 5, further comprising the step of generating a transaction message using said PIN block and said transaction data.

7. The method of claim 6, further comprising the step of sending said transaction message to a financial network.

8. The method of claim 1, wherein said hardware security module generates a PIN using said corollary data and said HSM data.

9. The method of claim 8, wherein said PIN block includes an encrypted PIN.

10. The method of claim 9, wherein said encrypted PIN is encrypted using a split-knowledge key.

11. A system for secure PIN processing comprising:

a transaction manager;

a transaction module communicably connected to said transaction manager;

a hardware security module communicably connected to said transaction manager;

wherein said transaction manager sends terminal data to said transaction module such that the transaction module generates corollary data using said terminal data and user input data and said transaction manager sends said corollary data and HSM data to said hardware security module, such that the hardware security module generates a PIN block using said corollary data and said HSM data.

12. The system of claim 11, wherein said transaction manager is communicably connected to said transaction module by an open network.

13. The system of claim 11, wherein said transaction manager is communicably connected to said hardware security module by a direct connection.

14. The system of claim 11 wherein said user input data comprises cursor location data.

15. The system of claim 11 wherein said terminal data includes an algorithm.

16. The system of claim 11 wherein said HSM data includes an algorithm.

17. The system of claim 11, further comprising a financial network, wherein said transaction manager sends a transaction message including said PIN block to said financial network.

18. The system of claim 17, wherein said financial network sends an authorization to said transaction manager in response to said transaction message.

19. The system of claim 11, further comprising a merchant server communicably connected to said transaction module and said transaction manager.

20. The system of claim 11, further comprising a terminal, wherein said transaction module is executed by said terminal.